

THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

PAIGE A. THOMPSON,

Defendant.

No. CR19-159-RSL

**REPLY IN SUPPORT OF MOTION
TO COMPEL PRODUCTION OF
CAPITAL ONE DATA**

Noted: January 14, 2022

The government’s arguments in opposition to defendant Paige Thompson’s motion to compel disclosure of Capital One data in the government’s possession pursuant to Federal Rule of Criminal Procedure 16 are meritless. The need for the Capital One data is paramount, and Rule 16 requires the government to permit Ms. Thompson to inspect and copy it.

Ms. Thompson is less than three months away from trial, and the government has not even produced the limited subset of Capital One data it says it intends to use in its case-in-chief to prove the multiple alleged crimes with which it has charged Ms. Thompson or the allegedly stolen data from the non-objecting victim entities.¹ (*See*

¹ On December 7, 2020, the government asked Ms. Thompson to provide an 8 terabyte (“TB”) hard drive so that it could send the data from the non-objecting alleged victim entities. (Dkt. 127-2, at 2.) Ms. Thompson provided the government with a 10 TB drive on December 15, 2021. (Exhibit 3, AUSA Letter.) As the Capital One data is less than

1 Dkt. No. 145 at 7 [discussing that it will introduce a subset of the data withheld from
2 the defense at trial].)

3 The government not only alleges that Ms. Thompson participated in a “scheme
4 and artifice” to access and copy “data that contained information, including personal
5 identifying information, from approximately 100,000,000 customers who had applied
6 for credit cards from Capital One,” (Dkt. No. 102 at ¶ 19), but that the value of the
7 information taken from Capital One “exceeded \$5,000,” (*Id.* at ¶ 24), Ms. Thompson
8 attempted to use the personal identifying information (“PII”) of “more than 15 Social
9 Security Numbers and more than 15 bank account numbers” stolen from Capital One
10 “to create counterfeit and unauthorized credit and debit cards,” (*Id.* at ¶ 32), and Ms.
11 Thompson “possessed, without lawful authority . . . the names and other [PII] of
12 millions of people.” (*Id.* at ¶ 34.) The government must prove all of these allegations
13 beyond a reasonable doubt at trial. Ms. Thompson is therefore absolutely entitled under
14 Rule 16 to inspect and copy the Capital One data to prepare her defense without being
15 monitored by the government (which may disclose its defense strategy) or having
16 defense access restricted by the hours and/or manpower of the FBI office where the
17 data is kept. Lastly, it bears repeating that the defense is willing to undertake
18 significant and proven safeguards to protect that data once it has a copy of it.

19 The Court should order the government to permit the defense to inspect and copy
20 the Capital One data pursuant to Rule 16.

21 //

22 //

23 //

24 _____
25 a TB of data, the government could provide it on the same drive as the other alleged
26 victims’ data. To date, the government has not returned the drive with the data. Also,
based on the discovery to date, the government has already made one copy of the data
in question and distributed it to Capital One.

I. Rule 16 and Case Law Support Ms. Thompson’s Demand for the Capital One Data.

Rule 16 is clear—"the government *must* permit the defendant to inspect *and* copy" data within the government’s possession, custody, or control that *either* (1) "was obtained from or belongs to the defendant" or (2) "the government intends to use the item in its case-in-chief at trial;" or (3) "is material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E) (emphasis added). In this case, the Capital One data in the government’s possession meets all three conditions, and thus the government must permit the defense to inspect and copy it.

A. The Capital One Data Must Be Produced to the Defense Because it Was Obtained from Ms. Thompson.

Contrary to the government’s assertion in its opposition, Rule 16 requires inspection and production not just where the data belongs to the defendant, but also where the data was obtained from the defendant. (Dkt. No. 145 at 7 ["Thompson also obviously cannot establish that the data at issue belongs to her[.]"]) Here, the government contends that the Capital One data was seized from Ms. Thompson as a result of a search warrant. This is not data the government obtained from Capital One itself.

The plain text of Rule 16 is quite clear—the government must permit inspection and copying if the data "was obtained from *or* belongs to the defendant." Fed. R. Crim. P. 16(a)(1)(E)(iii); *see, e.g., United States v. Mayer*, No. 19-CR-0096 (WMW/HB), 2020 WL 814187, at *6 (D. Minn. Feb. 19, 2020) (holding that defendant was entitled to inspect and copy all data seized from him except for alleged child pornography); *United States v. Roybal*, 46 F. Supp. 3d 1127, 1173 (D.N.M. 2014) (ordering government to produce financial documents taken from defendant’s home); *United States v. Rosas*, No. DR:13-CR-00173-DAE, 2013 WL 1345513, at *2 (W.D. Tex. Apr.

1, 2013) (finding defendant had right pursuant to Rule 16(a)(1)(E)(iii) to inspect and re-weigh cocaine seized from him even though he had no legal right to possess it).

The government's opposition also makes it appear as if production of the Capital One data to the defense will result in Ms. Thompson somehow disseminating the data to the public at large. (*See, e.g.*, Dkt. 145 at 8.) Such insinuations are unsupported to say the least, especially given the diligent manner in which the defense has stated it will handle the material. The Court should discount the government's claims and order the Capital One data to be produced or, alternatively, to be immediately available for the defense to inspect and copy.

B. The Capital One Data Must Be Produced to the Defense Because the Government Intends to Use the Data in its Case-in-Chief at Trial.

The government admits in its briefing that it intends to use "small, redacted, representative examples of the stolen data entries" found in the withheld Capital One data. (*Id.* at 7.) Yet, the government also admits that it has never produced *any* of the data. (*Id.* at 4.)

Rule 16 is clear—upon request by the defendant, which the government admits Ms. Thompson has made, (*id.* at 4), the government *must* permit the defendant to inspect and to copy the data if the government "intends to use the item in its case-in-chief at trial." Fed. R. Crim. P. 16(a)(1)(E)(ii). Given that the government intends to use the Capital One data in its case-in-chief, the government must permit Ms. Thompson to copy it.

To be frank, the defense cannot rely on the government to produce even the subset of Capital One data it intends to introduce at trial in a timely manner. It is now less than three months from trial, and the government has failed to produce that subset of data, and has not produced any of the data allegedly stolen by the other victim entities even though it agreed to do so, and even though those entities do not object to

1 the disclosure to Ms. Thompson. This lack of disclosure is why the defense needs the
 2 Court's intervention to protect Ms. Thompson's constitutional right to a fair trial.
 3 Such weighty constitutional concerns takes far greater precedence than Capital One's
 4 (and, apparently, the government's) unsupported belief that providing a copy of the data
 5 to the defense, to be hosted on a server disconnected from the Internet and behind
 6 multiple firewalls that has no record of ever having been hacked, could cause further
 7 harm, especially considering that Capital One has previously represented to the
 8 Honorable Anthony J. Trenga that "only a small fraction of the approximately 100
 9 million consumers impacted . . . had their SSNs and bank account information stolen."
 10 *Capital One's Memorandum of Law in Support of Its Motion to Dismiss the*
 11 *Representative Consumer Class Action Complaint* at 16, *In Re: Capital One Consumer*
 12 *Data Security Breach Litigation*, MDL No. 1:19-md-2915-AJT-JFA, (E.D.Va. April 10,
 13 2020). According to Capital One, the "other roughly 99.8% of the affected population
 14 had less sensitive information impacted" that "cannot alone be used to commit identity
 15 theft." (*Id.*) If that is a true statement, then there is little to no real risk to producing it
 16 to the defense, and the Court should grant the motion to compel.

17 **C. The Capital One Data Must Be Produced to the Defense Because it is**
 18 **Material to Preparing Ms. Thompson's Defense.**

19 The government's claim about materiality should be rejected. (*See* Dkt. No. 145
 20 at 6-7.) They do not withstand scrutiny.

21 Materiality is "a low threshold" which is satisfied so long as the information
 22 sought "would have helped to prepare a defense," even if that is to "simply cause[] a
 23 defendant to 'completely abandon' a planned defense and 'take an entirely different
 24 path.'" *United States v. Pacific Gas & Electric Co.*, No. 14-CR-00175-TEH, 2015 WL
 25 3958111, at *1 (N.D. Cal. Jun. 29, 2015) (quoting *United States v. Hernandez-Meza*,
 26 720 F.3d 760, 768 (9th Cir. 2013)). The materiality of requested evidence is only

1 scrutinized by the courts “more closely when it appears that production would impose
2 an undue burden on the [g]overnment.” *Id.* at *3.

3 As outlined in the motion to compel, the materiality of the Capital One data is
4 patently clear. (*See* Dkt. No. 127 at 1-5.) Moreover, the government has not, and
5 cannot, make a credible argument here that production of the Capital One data would
6 impose an undue burden. Indeed, the defense has already incurred some of the cost and
7 burden of making a forensic copy of the data by providing the government with a 10
8 TB drive and as soon as the Court orders the government to make it available for
9 copying, the defense will obtain a copy of the full data.

10 The only “significant” case the government uses to justify its decision to
11 withhold production of the Capital One data from the defense and, instead, require its
12 inspection at the FBI office is *Pacific Gas & Electric*, 2015 WL 3958111 (N.D.Cal.
13 2015), which is a wholly inapposite case. (*See* Dkt. No. 145 at 9-10.) In *Pacific Gas*
14 *& Electric*, the district court’s decision rested on Rule 16(a)(1)(B), *not* Rule
15 16(a)(1)(E). The provisions are textually different. Rule 16(a)(1)(B) requires only that
16 the government “disclose to the defendant, and make available for inspection, copying,
17 or photograph” the defendant’s written or record statement. Thus, requiring the defense
18 to review and copy a set of agent notes at a government office is fully within the textual
19 boundaries of the Rule. Further, to be clear, in that case, the defense could have copied
20 *all* of the witness notes had it wanted to do so. In contrast, Rule 16(a)(1)(E) requires
21 the government to “permit the defendant to inspect *and* to copy . . . data” that is
22 “material to preparing the defense;” “the government intends to use . . . in its case-in-
23 chief at trial;” or “the item was obtained from . . . the defendant[.]”

24 Certainly, requiring the defense to send a person to the FBI office to make a
25 forensic copy of the Capital One data is within the textual boundaries of Rule
26 16(a)(1)(E), but the government is not permitting such. Instead, the government wants

the defense to disclose its trial strategies by traveling to the FBI office at the FBI's convenience and identifying to the government which portions of the Capital One data it believes may be relevant to its defense (which may evolve over time and result in repeated visits, including during trial). That is *not* within the textual boundaries of Rule 16, it runs afoul of Ms. Thompson's constitutional rights, and it is most definitely not addressed in the *Pacific Gas & Electric* case.

D. The Court Has Already Regulated the Discovery at Issue Through the Issuance of Protective Orders and No Further Regulation is Necessary.

Rule 16(d)(1), entitled "Protective and Modifying Orders," permits the Court "for good cause" to "deny, restrict, or defer discovery or inspection, or grant other appropriate relief." Fed. R. Crim. P. 16(d)(1). The Court has already entered multiple protective orders in this case which protect the Capital One data. Thus, the government's further restrictions on the data, namely, holding the data at an FBI office to which the defense has no access outside of that granted by the government, during the FBI office's hours of operation and status (which may further be impacted due to the Omicron variant), and monitored such that any potential visit with a testifying expert could reveal defense strategy is not only wholly unnecessary, but antithetical to Ms. Thompson's constitutional rights. *See, e.g., United States v. Rounbehler*, No. 10-2634-MJ, 2011 WL 13290275, at *2 (D.N.M. Jan. 28, 2011) (compelling production of non-sexually explicit photos and videos defendant surreptitiously took of children and their parents because protective order adequately covered government's concern about sensitive materials and materials were "obtained from" defendant).

The government's suggestion that should Ms. Thompson wish "to preserve the secrecy of her testifying expert at trial" (*i.e.* should Ms. Thompson elect to preserve her constitutional right to a fair trial and follow the Federal Rules of Criminal Procedure) "[Ms.] Thompson could retain or send a different person to do this" is as impractical as

1 it is an unwarranted taxpayer burden. First, given the nature of the data, Ms.
 2 Thompson's defense is best prepared by having *both* defense counsel and any retained
 3 expert(s) review the data. (*See* Dkt. No. 145 at 5.) Although defense counsel is
 4 technologically savvy, counsel may miss connections in the data material to preparing
 5 Ms. Thompson's defense to the multiple charges for which the government plans to use
 6 the data (namely, wire fraud, computer fraud and abuse, access device fraud, and
 7 aggravated identity theft) that an expert will not miss. Second, as the government
 8 knows, Ms. Thompson is indigent and cannot afford her own counsel. The
 9 government's suggestion that Ms. Thompson hire a consulting expert in addition to a
 10 testifying expert just to be able to get access to data that was (a) seized from her; (b) is
 11 material to the defense; and (c) which the government intends to introduce in its case-
 12 in-chief demonstrates not only wholesale disregard for Rule 16, but also for the costs
 13 already being borne by the public in this case.

14 The government also has failed to show why the Federal Public Defender's plan
 15 to safeguard the materials—storing them on a computer with no access to the Internet
 16 and safely ensconced behind multiple firewalls—provides any less protection than its
 17 plan to house the data with the FBI. As the government admits, “we live in an age in
 18 which no defense is impermeable to cybercriminals.” (*See* Dkt. No. 145 at 7-8.)

19 As everyone knows, government servers have been hacked numerous times,
 20 leading to the dissemination of personal and confidential information.² The

22 ² *See, e.g.,* E. Roth, *The FBI's emails system was hacked to send out fake cybersecurity*
 23 *warnings*, The Verge (Nov. 14, 2021), *available at*
 24 [https://www.theverge.com/2021/11/14/22781341/fbi-email-system-hacked-fake-](https://www.theverge.com/2021/11/14/22781341/fbi-email-system-hacked-fake-cybersecurity-warnings)
 25 [cybersecurity-warnings](https://www.theverge.com/2021/11/14/22781341/fbi-email-system-hacked-fake-cybersecurity-warnings); A. Suderman and E. Tucker, *Justice Department says Russians*
 26 *hacked federal prosecutors*, AP News (Jul. 30, 2021), *available at*
[https://apnews.com/article/technology-europe-russia-election-2020-](https://apnews.com/article/technology-europe-russia-election-2020-5486323e455277b39cd3283d70a7fd64)
[5486323e455277b39cd3283d70a7fd64](https://apnews.com/article/technology-europe-russia-election-2020-5486323e455277b39cd3283d70a7fd64); E. Lichtblau, *Hackers Get Employee Records*
at Justice and Homeland Security Depts., N.Y. Times (Feb. 8, 2016), *available at*

government has pointed to no specific security flaw in the defense's plan, other than hyperbole,³ has not demonstrated any recent attack (or pattern of such) on the Federal Public Defender's network,⁴ and cannot demonstrate that Capital One's data would be any less subject to dissemination if housed at the FBI. Given these circumstances, and the plain language of Rule 16, the defense requests that the data be copied and provided to it (or be made immediately available for inspection and forensic copying by the defense), who will handle it pursuant to the procedures outlined in its initial motion.

II. Conclusion

For all the above reasons and those in Ms. Thompson's underlying motion, the Court should grant the motion to compel.

DATED this 7th day of January, 2022.

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI

/s/ Christopher Sanders
CHRISTOPHER SANDERS

/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

<https://www.nytimes.com/2016/02/09/us/hackers-access-employee-records-at-justice-and-homeland-security-depts.html>.

³ Neither the government (nor Capital One in its separate motion under the Crime Victims' Rights Act [Dkt. No. 147]) make any factual showing that turning over the data to the defense as required by Rule 16 would run afoul of any court order or subject Capital One to any type of sanction.

⁴ Defense counsel is not aware of any attack, recent or otherwise, on the Federal Public Defenders' network, and a Google search for such revealed no relevant news articles.

1 */s/ Brian Klein*
2 BRIAN KLEIN

3 */s/ Melissa Meister*
4 MELISSA MEISTER
5 Waymaker LLP

6 Attorneys for Paige Thompson
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26